



AF / ifw

CERTIFICATE OF MAILING BY FIRST CLASS MAIL

I hereby certify that this document is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date set forth below.

[Signature]

by Renee D. East

Date of signature and deposit - September 5, 2006

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Benjamin J. Parker et al)	Group Art Unit: 2155
)	
Serial No.: 10/054,103)	Confirmation No.: 3674
)	
Filed: 10/25/2001)	Examiner: Kevin T. Bates
)	
For: Configuration Recovery After)	Attorney Docket: 1689(15724)
Gateway Failure)	

09/11/2006 HWOLDGE1 00000039 210765 10054103

01 FC:1402 500.00 DA

APPELLANT'S BRIEF ON APPEAL

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the final rejection of the Examiner dated April 25, 2006, rejecting claims 1-7.

REAL PARTY IN INTEREST

The real party in interest in the present appeal is Sprint Communications Company L.P., assignee of the entire right, title, and interest in the present application.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to appellant, the appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

STATUS OF CLAIMS

The status of the claims is as follows:

Claims allowed: none.

Claims objected to: none.

Claims rejected: 1-7.

Claims withdrawn: none.

The claims being appealed are: 1-7.

STATUS OF AMENDMENTS

No amendment was filed after final rejection.

SUMMARY OF CLAIMED SUBJECT MATTER

Internet service provider (ISP) networks include a hub or gateway that functions as a concentrator or aggregator connected to a plurality of remote users. The gateway routes user traffic to destinations in the local network or to the external Internet. The gateway often functions as a service selection gateway (SSG) which allows users to connect to various subscribed, on-demand network services provided by the ISP, e.g., video on-demand servers, voice services, or firewall services (specification page 1, lines

10-20). To ensure that only paying subscribers gain access to the network, an authentication of the user is performed using an ID and password. Once a user is authenticated, the gateway is configured to interact with the user according to their user profile of subscribed services (page 1, lines 25-35). The authentication information (e.g., user ID and password) and the subscription information for the user are kept separately from the gateway itself in a centralized authentication, authorization, and accounting (AAA) server. Once a user establishes an authenticated connection session, some of this information is cached on the gateway to facilitate gateway operation without repeated access to the AAA server (page 1, line 35 to page 2, line 5). Thus, the gateway can operate at a higher throughput and the AAA server (which typically handles many gateways simultaneously and which also has the task of recording the length of time a user is logged-on to any pay for use service) is not overburdened.

Even though the gateway is the device that interacts with the user, it is the AAA server that is more critical for proper network operation. Therefore, the AAA server is typically provided with backup power systems and redundant hardware so that AAA functions are normally uninterrupted. Gateways, on the other hand, are much more likely to fail since the greater number of gateways present in a network would require an undesirably high investment in redundancy and power backup (page 2, lines 10-20). In prior networks, when a gateway fails the memory cache of user information stored in the gateway is lost. Since the authentication and user information is no longer available within the gateway when operation of the gateway is re-established, the user is required to re-authenticate by providing their user ID and password. This is undesirable due to the inconvenience to the user and due to the possibility of double billing to the user (page 2, lines 21-31).

As recited in claim 1, the present invention permits recovery of a gateway after a gateway failure in a manner that does not require a user to re-authenticate. More specifically, a method of managing user connection sessions with a gateway in a

computer network comprises storing user data on the gateway in response to authentication by the user (page 6, lines 25-34; and step 33 in Figure 5). In addition, user status information is stored in a table in a RADIUS server during times that an authenticated user session is established with the gateway (page 8, lines 23-38; and step 45 in Figure 5). The RADIUS server is on a physically separate machine than the gateway and is connected to the gateway via the computer network (AAA server 17 in Figure 4). The user status information is deleted from the table when the authenticated user session is terminated (page 7, lines 35-37). The gateway routes the user traffic in response to the user data (page 6, line 34 to page 7, line 2; and step 35 in Figure 5). A failure of the gateway is detected wherein the stored user data is lost (page 8, lines 1-20; and step 47 in Figure 5). The gateway sends a request to the RADIUS server to provide the user status information and user data corresponding to each user in the table (page 10, lines 3-7; and step 63 in Figure 7). The user data is then stored again on the gateway (page 10, lines 7-10; and step 64 in Figure 7). The gateway routes the user traffic to continue the authenticated user session in response to the user data and the user status information without requiring re-authentication following the failure (page 9, lines 10-12; and step 49 in Figure 5).

None of the claims contain either a means plus function or a step plus function element.

GROUND OF REJECTION TO BE REVIEWED

1. Whether claims 1-6 are unpatentable under 35 U.S.C. §103(a) over Sitaraman in view of Middledorp.
2. Whether claim 7 is unpatentable under 35 U.S.C. §103(a) over Sitaraman in view of Middledorp and further in view of Zhang.

ARGUMENT

Rejection of Claims 1-6 under 35 USC 103(a)

Claims 1-6

Independent claim 1 recites a method of managing user connection sessions with a gateway wherein user status information is stored in a table in a separate RADIUS server during times that an authenticated user session is established with the gateway. During recovery after a failure of the gateway, the gateway sends a request to the RADIUS server to provide the user status information and user data corresponding to each user in the table. The user data is re-stored on the gateway so that the gateway routes user traffic to continue the authenticated user session in response to the user data and the user status information without requiring re-authentication following the failure.

Sitaraman et al provides a network system for managing dynamic IP address assignment. An AAA service which may include the RADIUS protocol is used by Sitaraman to determine whether a user attempting to log in is authorized to obtain an IP address (col. 7, line 58 to col. 8, line 4). As stated at col. 7, lines 7-9, the “AAA service 10 is implemented in a computer, preferably the same machine or server as that of the protocol gateway 4...” Sitaraman fails to either teach or suggest maintaining user data on a gateway for routing user traffic according to authenticated user sessions, storing the user data in a RADIUS server which is physically separate from the gateway, and restoring the user data from the RADIUS server to the gateway after a gateway failure. The equally viable possibility of the components of Sitaraman being on two different machines does not lead to the conclusion that Sitaraman suggests the invention of claim 1. Rather, the fact that Sitaraman functions equivalently whether its two functions are on the same machine or on different machines is proof that Sitaraman is not performing the functions recited in claim 1 which can only be performed by two separate machines.

It is clear from claim 1 that an authenticated user session is established with the gateway based on user data stored in the gateway. At that time, user status information is also stored in the RADIUS server. Prior to a failure, the gateway routes user traffic in response to the user data. After a failure of the gateway in which the user data for routing traffic is lost, the user data is restored on the gateway from the RADIUS server to continue the authenticated user session without requiring re-authentication following the failure. Whether or not Sitaraman uses one or two machines, nothing in its disclosure is suggestive of a redundant storage of user data for authenticated user sessions on another machine. Although Sitaraman backs-up information for a database of allocated IP addresses, this also is not suggestive of the claimed method of managing user connection sessions that stores user data on the gateway in response to authentication by the user and that stores user status in the RADIUS server. Storage of an IP address allocation is insufficient to establish the information needed to continue an already authenticated session between the user and the gateway. In particular, nothing in Sitaraman suggests any method that would allow a gateway to continue an authenticated user session without requiring re-authentication following a failure of the gateway.

The addition of Middledorp fails to strengthen the rejection. Middledorp does not relate to user authentication at all. It discloses a network of computer nodes of a process system, i.e., a process employed to produce amounts of a desired products using vats, transfer lines, machinery and the like (column 1, lines 11-19). The host processor and various workstations of Middledorp are part of a closed system wherein no particular individual users are identified at each workstation. Middledorp does not place security barriers between workstations and does not authenticate any users. Instead, Middledorp uses gateways as interpreters between various potentially-incompatible computer programs. Since Middledorp lacks storage of any user data, it likewise cannot request user status or user data after failure of a gateway. Thus, the combination of Sitaraman

and Middledorp fails to teach or suggest the invention as claimed in independent claim 1 or its dependent claims 2-6.

In view of the actual teachings of the references, it is readily apparent that besides the fact that the combined references fail to produce the claimed limitations, there is no motivation to combine the references as proposed and no motivation to modify the combined references to produce the claimed limitations.

Rejection of Claim 7 under 35 USC 103(a)

Claim 7

Claim 7 stands or falls together with its base claim 1. Since Zhang fails to correct for the deficiencies of Sitaraman and Middledorp, claim 7 is likewise allowable.

CONCLUSION

The final rejection has failed to establish a case of prima facie obviousness of any of claims 1-7. The prior art relied upon in the final rejection neither teaches nor suggests the structure or function of the present invention nor does it provide any teaching which can obtain the significant advantages which are achieved by the present invention. Accordingly, the rejection contained in the final rejection dated April 25, 2006, should be reversed.

Respectfully submitted,



Mark L. Mollon
Registration No. 31,123
Attorney for Appellant

Date: September 5, 2006
MacMillan, Sobanski & Todd, LLC
One Maritime Plaza, Fifth Floor
720 Water Street
Toledo, Ohio 43604
Tel: 734-542-0228
Fax: 734-542-9569

CLAIMS APPENDIX

Claims 1-7 now read as follows:

1. A method of managing user connection sessions with a gateway in a computer network, said method comprising the steps of:
 - storing user data on said gateway in response to authentication by said user;
 - storing user status information in a table in a RADIUS server during times that an authenticated user session is established with said gateway, said RADIUS server being on a physically separate machine than said gateway and being connected to said gateway via said computer network;
 - deleting said user status information from said table when said authenticated user session is terminated;
 - said gateway routing said user traffic in response to said user data;
 - detecting a failure of said gateway wherein said stored user data is lost;
 - said gateway sending a request to said RADIUS server to provide said user status information and user data corresponding to each user in said table;
 - storing said user data on said gateway; and
 - said gateway routing said user traffic to continue said authenticated user session in response to said user data and said user status information without requiring re-authentication following said failure.
2. The method of claim 1 wherein said user status information includes an IP address assigned to said user for said session.
3. The method of claim 1 wherein said detecting step is comprised of a power-up initialization.

4. The method of claim 1 wherein said step of requesting said RADIUS server to provide said user status information and said user data is included in a boot-up sequence of said gateway.

5. The method of claim 1 wherein said user data comprises a host object and a connection object.

6. The method of claim 5 wherein said step of storing user status information in said table is delayed until a connection object is created for said user.

7. The method of claim 1 wherein said gateway is comprised of a service selection gateway.

EVIDENCE APPENDIX

No evidence has been submitted under 37 CFR §§1.130, §§1.131, §§1.132, or otherwise.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings and no corresponding decisions rendered.



FEE TRANSMITTAL For FY 2006

Effective 12/08/2004. Fee pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

Complete if known

Application Number	10/054,103
Filing Date	10/25/2001
First Named Inventor	Benjamin J. Parker et al.
Examiner Name	Kevin T. Bates
Art Unit	2155
Attorney Docket No.	1689(15724)

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT

(\$ 500.00)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account: Deposit Acct. Number: 21-0765 Deposit Acct. Name: Sprint Communications Company L.P.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☒ Charge fee(s) indicated below

☐ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)
under 37 CFR 1.16 and 1.17

☐ Charge fee(s) indicated below, except the filing fee to the
above-identified deposit

Warning: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description

Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent
Multiple dependent claims

	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims _____ Extra Claims _____ Fee (\$) _____ Fee Paid (\$) _____

Multiple Dependent Claims
Fee (\$) _____ Fee Paid (\$) _____

HP = highest number of total claims paid for, if greater than 20

Indep. Claims _____ Extra Claims _____ Fee (\$) _____ Fee Paid (\$) _____

HP = highest number of total claims paid for, if greater than 3

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets _____ Extra Sheets _____ Number of each additional 50 or fraction thereof _____ Fee (\$) _____ Fee Paid (\$) _____

4. OTHER FEE(S)

Non-English Specification, \$130 fee (no small entity discount)
Other: 1402 - 500.00

SUBMITTED BY

(Complete (if applicable))

Name (Print/Type)	Mark L. Mollon	Registration No. (Attorney/Agent)	31,123	Telephone	(734) 542-0900
Signature				Date	September 5, 2006

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038. This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. If you need assistance in completing the form, call 1-800-PTO-9199 and select Option 2.